Amendments to the Specification

Please replace the specification on file with the replacement specification attached herewith. A marked up version and a clean version of the replacement specification are attached. Applicants have reviewed the specification and have attempted to correct all obvious errors found therein. The objection under 35 USC 112, second paragraph is believed to be overcome in view of the replacement paragraph. No new matter is believed to be added by the replacement specification.

09/807,697
PF980072
Substitute specification - Clean copy

COPY METHOD PREVENTING BIT-TO-BIT DUPLICATION OF DIGITAL DATA AND READING DEVICE FOR IMPLEMENTING SAME

This application claims the benefit of French application serial no. 98/13074 filed October 19, 1998, and which claims the benefit under 35 U.S.C. § 365 of International Application PCT/FR99/02425, filed October 11, 1999, which was published in accordance with PCT Article 21(2) on April 27, 2000 in French.

The present invention relates to a method of copying which prevents bit-by-bit duplication of digital data from a first source on a medium. It also relates to a device used to implement this method.

Digital data exhibit the property of being able to be copied without appreciable loss of quality. Indeed, copying consists in transmitting a series of binary information, namely "1"s and "0"s from the source to the recorder device. The errors which customarily occur during copying are easily corrected by using well known error correction methods. Thus, when an information medium or a data source contains digital data, it is relatively simple to record them identically on a recordable medium.

To protect digital data against illicit copying, various methods are used.

Usually, the supplier furnishes the digital data medium such as the diskette in the case of software, with a mark preventing any copying.

In the document EP-A-0 773 490, there is proposed a system for protecting the information stored in recording media, in which system each medium comprises an identifier.

Another way of protecting digital data against copying consists in endowing them with a watermark or "tattoo", that is to say with auxiliary data tied to

the digital data. The watermark must be non-modifiable and non-erasable. In this case, the reading of the data is done with the aid of a private key which identifies the watermark. Should there be any copying of the watermarked digital data, a private key is required to put the watermark back in place on the copy, without which the copy becomes illegal, as it is devoid of watermark. The digital data copied without watermark are no longer read by the reader since the latter does not identify the watermark where it ought to find one. Thus, the watermark precludes any copying without the private key.

These known methods of protecting copies are in general effective when the medium is processed by compliant reading or recording apparatuses. However, these methods do not prevent duplication by a pirate who creates a double or clone which is as similar as possible to the original by carrying out what is termed bit-by-bit copying.

The aim of the present invention is to propose a method of copying which prevents unauthorized duplication of digital data arising from a first source on a medium, this method preventing bit-by-bit copying of the digital information.

The aim of the present invention is also to provide a reading device comprising circuits allowing the implementation of said method.

Accordingly, the subject of the present invention is a method of copying which prevents bit-by-bit duplication of digital data arising from a source of digital data on a medium. According to the invention, the method comprises a step of formatting the digital data arising from said source of digital data as a function of a serial number contained in said medium and a step of writing said formatted data onto said medium.

According to a preferred embodiment, the serial number is recorded in an unfalsifiable manner on the

medium during its manufacture. For maximum prevention of any pirating, the serial number is a unique number for each medium or exhibits a low probability of being common to two media.

Furthermore, the formatting of the digital data to be duplicated is carried out using a secret-key encryption algorithm such as DES or a public-key algorithm such as RSA, the encryption key being dependent on the serial number.

Preferably, the encryption key is moreover dependent upon a secret parameter which is contained in any reading device adapted for reading the digital data arising from said data source.

The present invention also relates to a method of copying which prevents bit-by-bit duplication of digital data read by a reading device and copied onto a medium, characterized in that the medium comprises a serial number and in that the method of copying comprises the following steps:

- sending the serial number recorded on the medium to the reading device,
- formatting the digital data read with the aid of the serial number, and
- recording on said medium the formatted digital data.

According to a preferred embodiment, the formatting step is carried out in the reading device. Said reading device furthermore comprises means for making it possible to read the medium containing the formatted digital data.

According to a further characteristic of the method in accordance with the present invention, before performing the duplication of the digital data, the method comprises a step of checking authorization to copy.

The present invention also relates to a reading device allowing the implementation of the said methods of copying described hereinabove. According to this

aspect of the invention, the device comprises a formatting circuit adapted for receiving the serial number of the medium onto which the digital data are to be copied and providing, as output, formatted data which are dependent on said serial number and are intended to be copied onto said medium.

The invention also relates, according to another aspect, to a recording medium for digital data comprising a serial number which is unique or exhibits a low probability of being common with that of another medium, characterized in that it furthermore comprises recorded digital data, said digital data being formatted as a function of said serial number and of a secret parameter.

Other characteristics and advantages of the present invention will become apparent on reading the description of a preferred embodiment given with reference to the herein-appended drawing in which:

Figure 1 is a diagrammatic view in block form of a reading device and of a recorder device allowing the copying of digital data from a first medium onto a second medium.

The present invention will be described whilst referring to the reading of digital data recorded on a digital medium such as a DVD standing for Digital Versatile Disc and copied onto a second virgin medium likewise consisting of a DVD which in this case must be recordable, namely a DVD-R. However, it is obvious to the person skilled in the art that other sources of digital information may be used, in particular digital information arising from a decoder and sent by a "broadcaster" or digital information stored on media such as a magnetic tape, a recordable or non-recordable optical disc, namely a CD, a CD-R, CD-RW, DVD, DVD-R, a magneto-optical disc or the like. The recording medium consists of a recordable magnetic tape, a CD-R, a CD-RW, a DVD-R or a magneto-optical disc allowing storage of the audio and/or video information in digital form.

As represented in figure 1, the method of copying in accordance with the present invention makes it possible to copy the digital information D recorded on a DVD 1 by using a reading device 2 furnished with a formatting circuit 3 and the data FD which may be duplicated are recorded on a DVD-R 4 inserted into a recorder device 5.

In accordance with the present invention, the DVD-R 4 consisting of a virgin DVD-R comprises a serial number which is recorded in an unfalsifiable manner during the manufacture of the DVD-R. This serial number which is chosen in such a way as to be unique or to exhibit a very low probability of being present on two different media, is stored in a concealed area of the disc, such as the area entitled the "lead-in area", namely the track lead-in. As explained in greater detail hereinbelow, this serial number is used to format the digital data read from the original DVD 1.

In accordance with the method claimed in the present invention, the data read on the DVD 1 by the reading device 2 are sent to a formatting circuit 3 which carries out a formatting of the data by using the serial number read on the virgin DVD-R. Data FD formatted in a specific manner are thus obtained at the output of the reading device and are sent to the recorder device 5 where they are recorded on the DVD-R 4.

To carry out a formatting of the data such that the data recorded on the DVD-R cannot be copied bit-by-bit but can however be read back subsequently by the reading device, namely to make a so-called licit copy, various formatting processes may be used. One of the conventional formatting processes is a secret-key encryption algorithm such as DES standing for "Data Encryption Standard" which is well known to specialists. To prevent any copying by a pirate, the key used in this case will be a key constructed with the aid of a secret key and of the serial number read

on the virgin DVD-R. To carry out the formatting using this algorithm, the data recorded on the original DVD are divided up into blocks of 64 bits then formatted by the DES using a 56-bit key obtained from the serial numbers. 64-bit formatted or enciphered data packets are obtained at the output and are recorded by way of the recorder apparatus 5 on the DVD-R 4. If the key consists of the serial number itself, the serial number will comprise 56 bits. However, the number of bits of the serial number is given by way of example. Indeed, it is possible to apply the invention to media whose serial numbers have lengths of greater than or less than 56 bits. In this case, a truncation or a channel coding can be applied so as to bring these serial numbers to the correct length. If the key is, for security reasons, a function of the serial number, it can be obtained as follows:

Given that NS is the serial number of the recording medium, and PS is the parameter stored in a secure manner in the compliant reading devices:

- NS and PS are concatenated so as to have a word (NS/PS),

- a hash function is applied such as the function SHA-1 (standard of the National Institute of Standards and Technologies) and this results in the word SHA (NS/PS) which has a length of 64 bits, and

- this word is truncated so as to have a 56-bit word which will serve as key for the DES.

The length of the binary words NS and PS is not fixed, since SHA-1 does not necessitate a precise length for the input word. The function f accommodates any length of serial number.

The DVD-R 4 thus copied licitly can be read by the reading device 2 and the original digital data are recovered using the corresponding decryption algorithm.

It is also possible to carry out the formatting of the digital data to be duplicated by using a public-key algorithm such as the RSA algorithm. This public-

key algorithm is an asymmetric algorithm which, when the public key is known, precludes easy copying of the formatted data during their reading by the reading device 2.

Since the data located on the copy DVD-R do not have the same structure as the data of the original DVD, it is therefore not possible to recover them with a reading device other than a compliant reading device. Moreover, if a bit-by-bit copy of the original DVD has been made, the reading device of the present invention does not retrieve the original digital information and will not read the copy.

According to a further characteristic of the present invention, the method of copying can be preceded by a step of checking authorization to copy. This checking of authorization to copy is applied to an information medium comprising a first identification of a cipher of the digital data, a second identification of a watermark of digital data, a first determination of a first mark if it has been possible to identify the cipher and the watermark, a third identification of a type of the information medium, a second determination of a second mark if it has been possible to determine the first mark and if it has been possible to identify a determined type of information medium, a fourth identification of cryptographic signature data accompanying the digital data, a third determination of a third mark if it has been possible to determine the second mark and if it has been possible to identify a cryptographic signature datum and a first delivery of permission for digital copying of the digital data if it has been possible to determine the third mark.

In accordance with the present invention, the device 2 for reading the digital data which may be a DVD reader, a decoder, a CD reader or the like, comprises a formatting circuit 3 consisting essentially of an integrated circuit including all the means required for carrying out the algorithm chosen for the

formatting and making it possible to store in an unfalsifiable manner certain data such as a secret key or means for authorizing copying.

The embodiment described hereinabove is given by way of example and can be modified without departing from the framework of the claims herein-enclosed.